ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Теоретические основы компьютерной безопасности

Экзаменационные материалы

Автор: профессор кафедры алгебры
и дискретной математики
Н.А. Гайдамакин

Екатеринбург
2008

Билет № **1**

1. История теории и практики компьютерной безопасности
2. Политика и зональная модель безопасности в распределенных КС

Задача.

Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа (**ТАМ**), имеется четыре типа сущностей (субъектов и объектов доступа) – ***u***, ***ν***, ***ω*** и ***ψ***.

Пусть в начальном состоянии системы имеется субъект s_1 типа ***u*** - (s_1: ***u***).

Осуществляется переход системы в новое состояние посредством команд α_1 и α_2:

α_1(s_1:***u***, s_2: ***ω***, o_1: ***ν***):

Create object o_1 ***of type*** ***ν*** **;**
Inter r into [s_1, o_1] **;**
Create subject s_2 ***of type*** ***ω*** **;**
Inter r′ into [s_2, o_1] **;**
end α_1

α_2(s_1:***u***, s_2:***ω***, o_2: ***ψ***):

Create object o_2 ***of type*** ***ψ*** **;**
Inter r″ into [s_1, o_2] **;**
Inter r‴ into [s_2, o_2] **;**
Create subject s_3 ***of type u*** **;**
Inter r⁗ into [s_3, o_1] **;**
end α_2

Задание.

Прокомментируйте действие команд α_1 и α_2 .

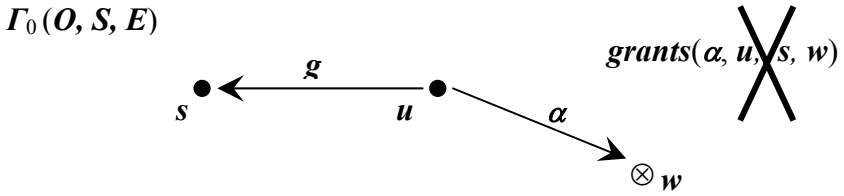
Постройте в два этапа по командам α_1 и α_2 граф отношений наследственности ***Γ***. Есть ли на графе ***Γ*** циклы длиной 3 и 4? Что означает с точки зрения безопасности наличие циклов на графе отношений наследственности?

Билет № **2**

1. Структура понятия компьютерная безопасность, основные способы и механизмы защиты информации в КС
2. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба

Задача.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$.



Установленная для системы политика безопасности запрещает любым субъектам (владельцам) предоставлять право α на "свои" объекты другим субъектам (но не запрещает субъектам, которые владеют правами ***t*** ("брать") на какие-либо субъекты, брать у них права на их объекты).

Кроме субъекта ***s***, субъект ***u*** может быть связан ***tg***-путем с другими субъектами.

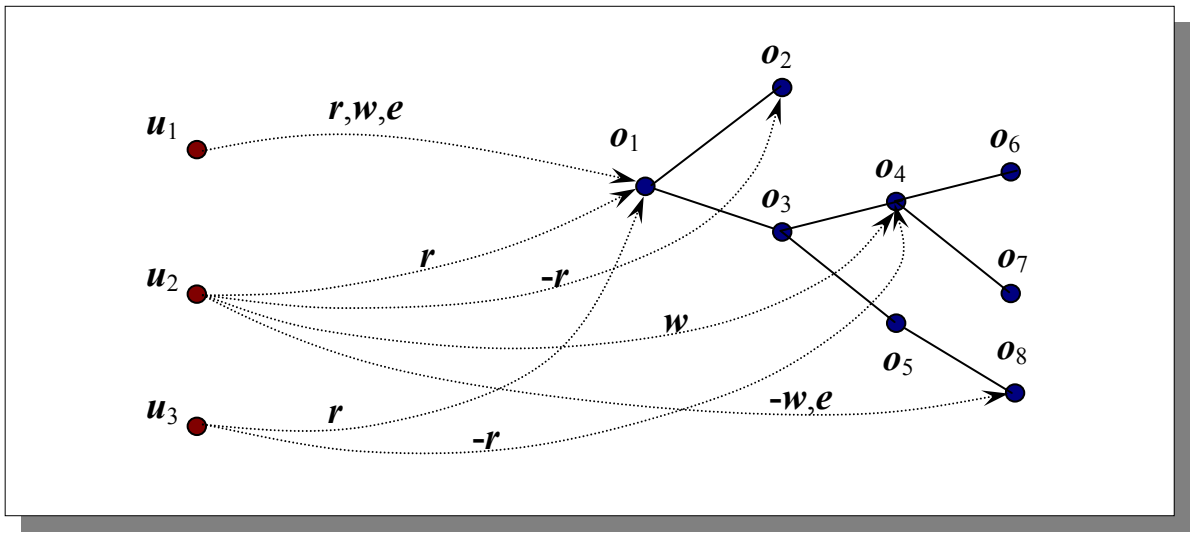
Задание: построить систему команд получения субъектом ***s*** прав доступа α на объект ***w*** от субъекта ***u***, при условии того, что команда ***grants***(α, ***u***, ***s***, ***w***) не может быть задействована.

Билет № **3**

1. Понятие защищенности (безопасности) компьютерной информации. Конфиденциальность, целостность и доступность информации
2. Основы политики мандатного доступа. Решетка безопасности.

Задача.

Пусть имеется иерархически организованная система объектов доступа и три пользователя u_1, u_2 и u_3. Назначения доступа показаны на рис.



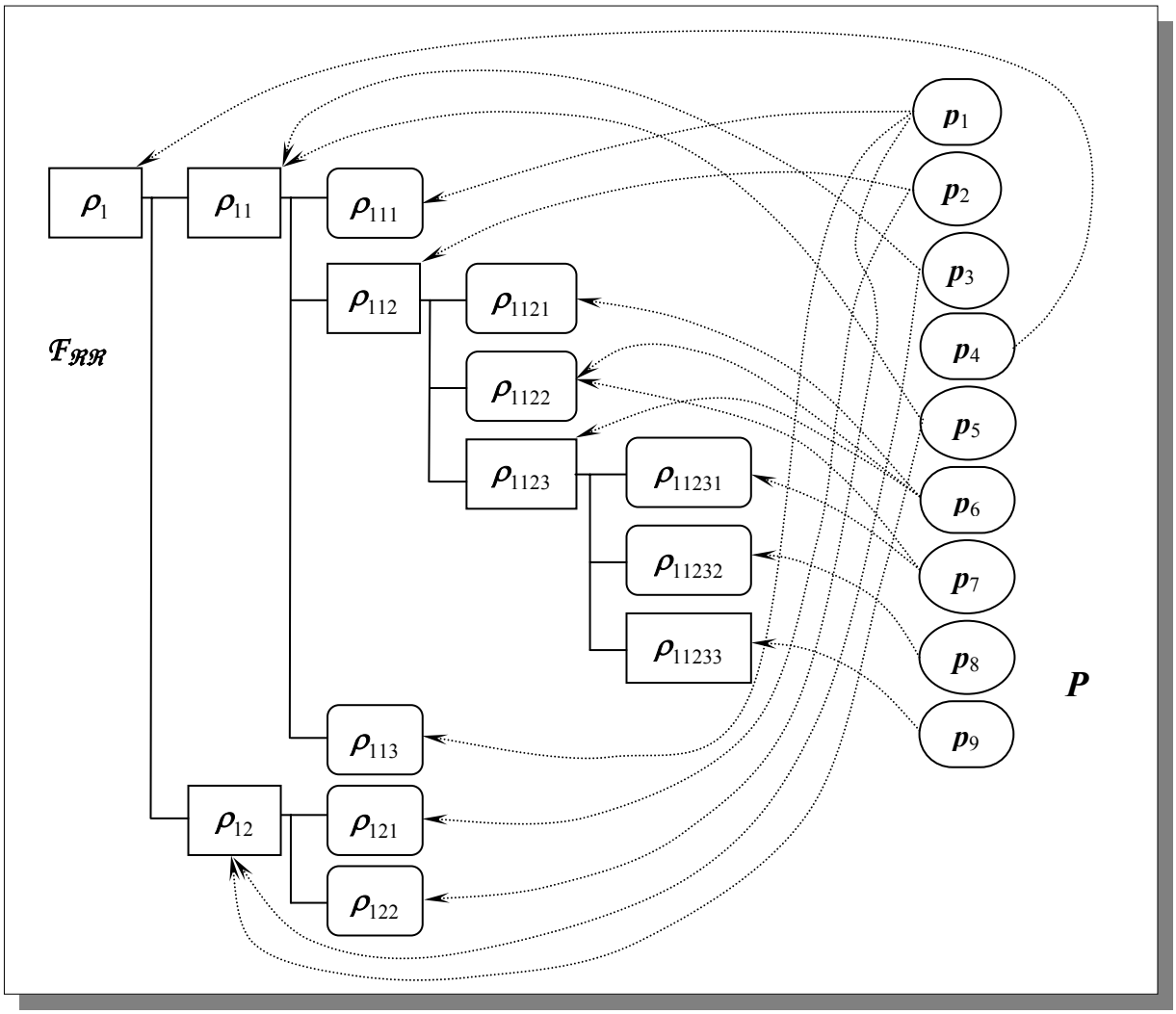
Задание. Приведите матричные соотношения и определите по ним итоговые права доступа пользователей по чтению и записи.

Билет № **4**

1. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
2. Методы, критерии и шкалы оценки эмпирических объектов.

Задача.

Пусть имеется система иерархически организованных ролей $\mathcal{R}$ ($\rho \in \mathcal{R}$), представленная на рис. Ролям назначены полномочия из конечного множества $\boldsymbol{P}$ ($\boldsymbol{p} \in \boldsymbol{P}$).



Задание. Определите тип наделения ролей полномочиями (листовой таксономический, листовой нетаксономический, иерархически охватный).

Определите полномочия роли ρ_{112}.

При предположении, что определенные полномочия могут быть назначены только ролям определенного уровня иерархии, определите возможный порядок (отношение доминирования) на множестве полномочий.

Билет № **5**

1. Понятие и таксонометрия угроз безопасности и изъянов (брешей) систем защиты.
2. Модель Белла-ЛаПадулы и основная теорема безопасности

Задача.

Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа **TAM**, имеется два субъекта доступа: субъект s_1 типа a - (s_1: a) доверенного пользователя (*admin*); субъект s_2 типа u - (s_2: a) обычного пользователя (*user*); а также три объекта доступа: каталог o_1 типа ν (*secret*) – (o_1: ν), владельцем которого является пользователь s_1 (*"own"*$\in r_{s_1,o_1}$), несекретный каталог o_2 типа η (*no secret*) – (o_2: η), владельцем которого является пользователь s_2 (*"own"*$\in r_{s_2,o_2}$), секретный файл o_3 типа ν – (o_3: ν) в каталоге o_1, владельцем которого также является пользователь s_1 (*"own"*$\in r_{s_1,o_3}$). Пользователь s_1 имеет также права *чтения*, *записи* и *запуска* на объект o_2 ({*"read","write","execute"*} $\subseteq r_{s_1,o_2}$).

В исходном состоянии Графа наследственности имеется четыре вершины.

Задание. Постройте Граф отношений наследственности по сценарию атаки троянским конем со стороны пользователя s_2 на секретный файл o_3. Прокомментируйте с точки зрения модели **TAM** полученный Граф отношений наследственности.

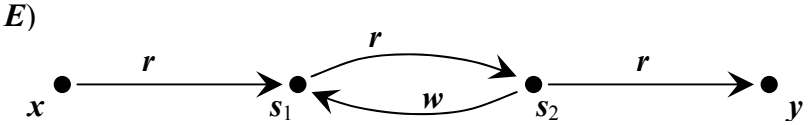
Билет № **6**

1. Монитор безопасности КС и гарантирование выполнение политики безопасности
2. Теоретико-графовые модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности.

Задача.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\boldsymbol{\Gamma}_0(\boldsymbol{O, S, E})$,

$\boldsymbol{\Gamma}_0(\boldsymbol{O, S, E})$



Пусть неявные каналы чтения, генерируемые различными командами "де-факто" имеют следующую стоимость: - $\boldsymbol{r}_{\mathbf{spy}} = 1$, $\boldsymbol{r}_{\mathbf{post}} = 2$, $\boldsymbol{r}_{\mathbf{find}} = 3$ и $\boldsymbol{r}_{\mathbf{pass}} = 4$.

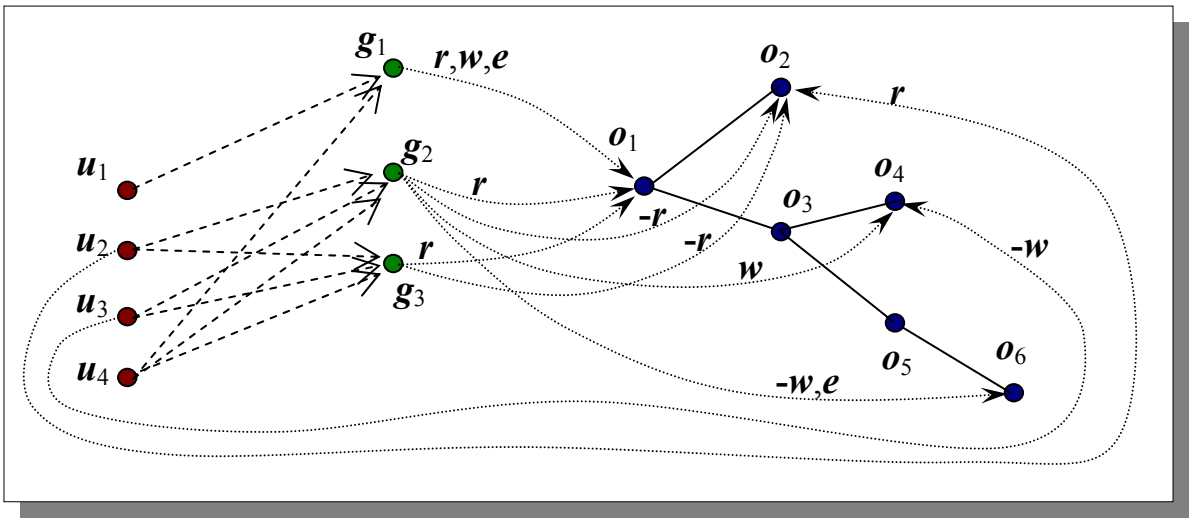
Задание: Применяя команды "де-факто", сгенерировать все возможные неявные каналы чтения субъектом $\boldsymbol{x}$ информации из субъекта $\boldsymbol{y}$, и сравнить их стоимость.

Билет № **7**

1. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах
2. Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.

Задача.

Пусть имеется иерархически организованная система объектов доступа, четыре пользователя $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, $\boldsymbol{u}_3$ и $\boldsymbol{u}_4$, объединенных в три рабочих группы $\boldsymbol{g}_1$, $\boldsymbol{g}_2$ и $\boldsymbol{g}_3$. Вхождение пользователей в рабочие группы, групповые и индивидуальные назначения доступа показаны на рис.



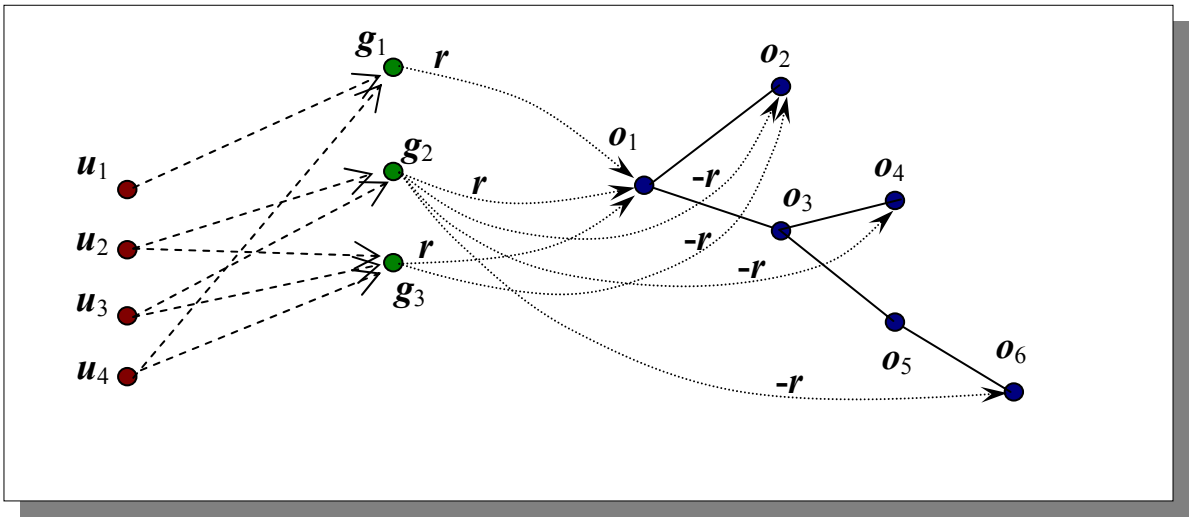
Задание. Приведите матричные соотношения и определите итоговые права доступа пользователей по чтению и записи.

Билет № **8**

1. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
2. Идентификация и оценка угроз безопасности

Задача.

Пусть имеется иерархически организованная система объектов доступа, четыре пользователя u_1, u_2, u_3 и u_4, объединенных в три рабочих группы g_1, g_2 и g_3. Вхождение пользователей в рабочие группы, групповые и индивидуальные назначения доступа показаны на рис.



Итоговые права доступа рабочих групп по чтению представлены следующей таблицей:

	o_1	o_2	o_3	o_4	o_5	o_6	
g_1	1	1	1	1	1	1	$R^r r\|_{итог}$
g_2	1	0	1	0	1	0	чтение
g_3	1	0	1	1	1	1	

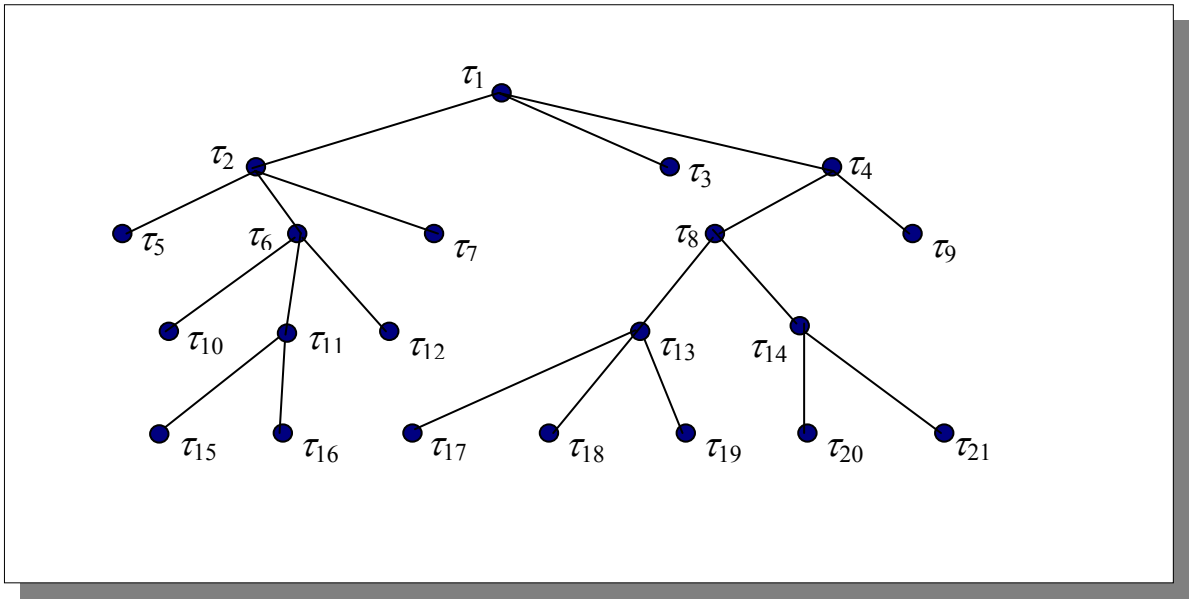
Задание. Приведите матричные соотношения и определите меры близости рабочих групп по вхождению в них пользователей и меры близости рабочих групп по правам на чтение.

Билет № **9**

1. Модели обеспечения целостности. Мандатная модель Кена Биба и ее разновидности
2. Системы многомерного шкалирования защищенности компьютерных систем

Задача.

Пусть имеется иерархический тематический рубрикатор.



Для тематической классификации сущностей системы (субъектов и объектов доступа) использованы наборы рубрик (мультирубрики):

I вариант

$\mathcal{T}^{M}_1 = \{\tau_6, \tau_7\}$; $\mathcal{T}^{M}_2 = \{\tau_{10}, \tau_{12}, \tau_{15}, \tau_{17}\}$; $\mathcal{T}^{M}_3 = \{\tau_{17}, \tau_{18}, \tau_{21}\}$; $\mathcal{T}^{M}_4 = \{\tau_3, \tau_4, \tau_6\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$;
$\mathcal{T}^{M}_6 = \{\tau_9, \tau_{13}\}$; $\mathcal{T}^{M}_7 = \{\tau_2, \tau_{14}, \tau_{16}\}$; $\mathcal{T}^{M}_8 = \{\tau_7, \tau_8, \tau_{21}\}$; $\mathcal{T}^{M}_9 = \{\tau_5, \tau_8, \tau_9\}$

II вариант

$\mathcal{T}^{M}_1 = \{\tau_6, \tau_7\}$; $\mathcal{T}^{M}_2 = \{\tau_{10}, \tau_{12}, \tau_{15}, \tau_{17}\}$; $\mathcal{T}^{M}_3 = \{\tau_{17}, \tau_{18}, \tau_{21}\}$; $\mathcal{T}^{M}_4 = \{\tau_3, \tau_4, \tau_6\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$;
$\mathcal{T}^{M}_6 = \{\tau_5, \tau_9, \tau_{13}\}$

Задание.

Все ли наборы рубрик в первом варианте являются мультирубриками?

Определите отношения доминирования (уже, шире, несравнимо) между следующими мультирубриками:

$\mathcal{T}^{M}_1$ и $\mathcal{T}^{M}_2$; $\mathcal{T}^{M}_3$ и $\mathcal{T}^{M}_4$; $\mathcal{T}^{M}_5$ и $\mathcal{T}^{M}_6$; $\mathcal{T}^{M}_2$ и $\mathcal{T}^{M}_4$.

Постройте объединение следующих мультирубрик по второму варианту:

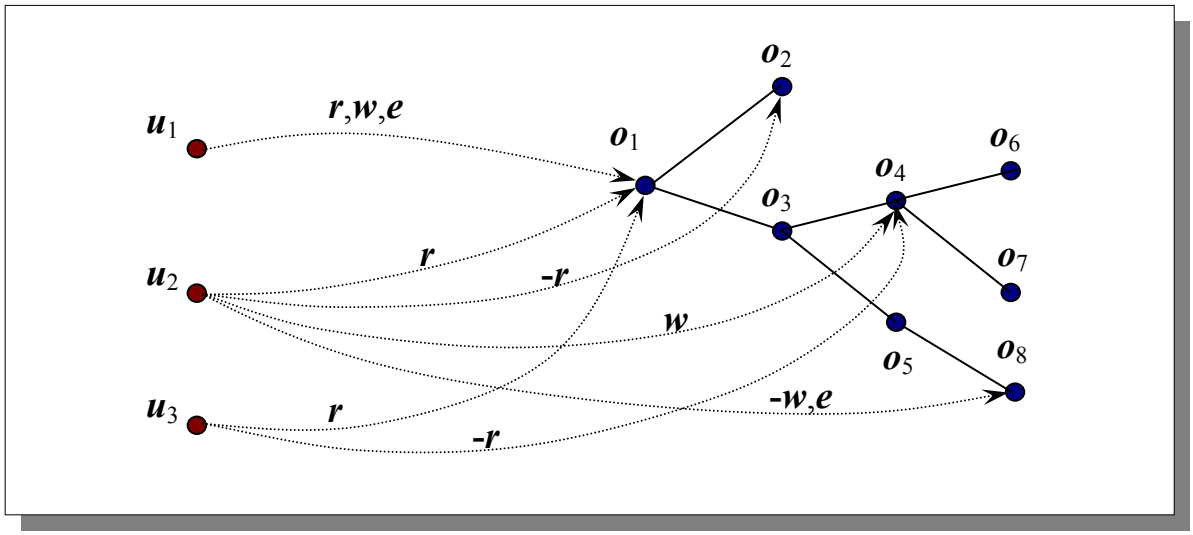
$\mathcal{T}^{M}_1 \cup_{M} \mathcal{T}^{M}_2$; $\mathcal{T}^{M}_2 \cup_{M} \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_4 \cup_{M} \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_1 \cup_{M} \mathcal{T}^{M}_6$

Билет № **10**

1. Модель TAKE-GRANT
2. Общая характеристика политики тематического разграничения доступа

Задача.

Пусть имеется иерархически организованная система объектов доступа и три пользователя u_1, u_2 и u_3. Назначения доступа показаны на рис.



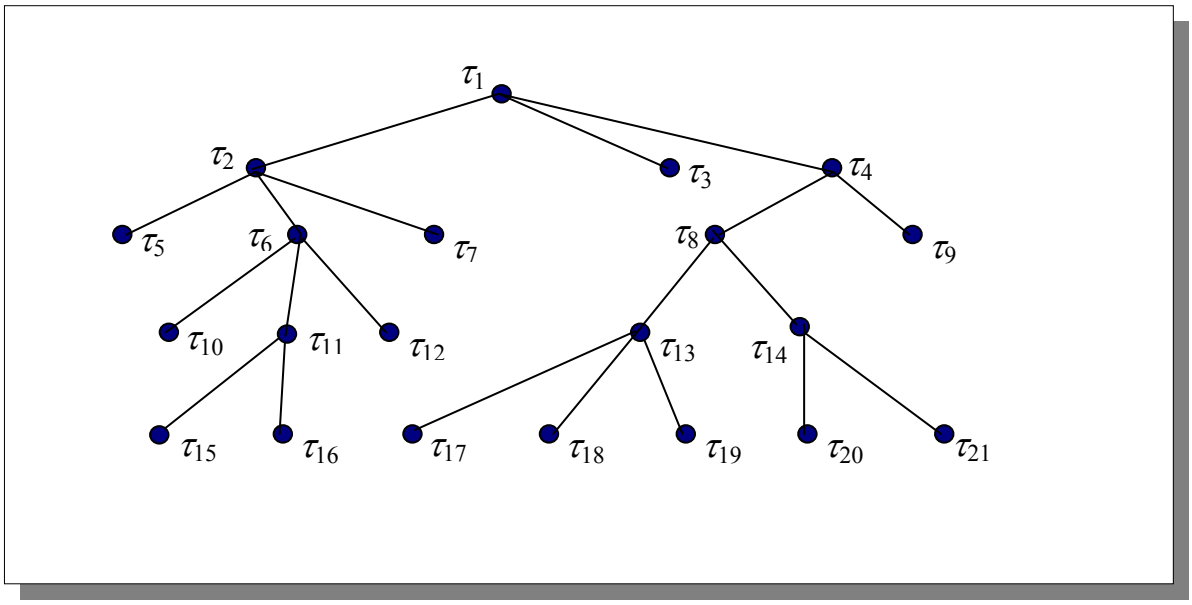
Задание. Приведите матричные соотношения и определите меры близости пользователей в пространстве доступа (по итоговым правам на запись).

Билет № **11**

1. Расширенная модель TAKE-GRANT
2. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах

Задача.

Пусть имеется иерархический тематический рубрикатор.



Для тематической классификации сущностей системы (субъектов и объектов доступа) использованы наборы рубрик (мультирубрики):

I вариант

$\mathcal{T}^{M}_1 = \{\tau_6, \tau_7\}$; $\mathcal{T}^{M}_2 = \{\tau_{10}, \tau_{12}, \tau_{15}, \tau_{17}\}$; $\mathcal{T}^{M}_3 = \{\tau_{17}, \tau_{18}, \tau_{21}\}$; $\mathcal{T}^{M}_4 = \{\tau_3, \tau_4, \tau_6\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$;
$\mathcal{T}^{M}_6 = \{\tau_9, \tau_{13}\}$; $\mathcal{T}^{M}_7 = \{\tau_2, \tau_{14}, \tau_{16}\}$; $\mathcal{T}^{M}_8 = \{\tau_7, \tau_8, \tau_{21}\}$; $\mathcal{T}^{M}_9 = \{\tau_5, \tau_8, \tau_9\}$

II вариант

$\mathcal{T}^{M}_1 = \{\tau_6, \tau_7\}$; $\mathcal{T}^{M}_2 = \{\tau_{10}, \tau_{12}, \tau_{15}, \tau_{17}\}$; $\mathcal{T}^{M}_3 = \{\tau_{17}, \tau_{18}, \tau_{21}\}$; $\mathcal{T}^{M}_4 = \{\tau_3, \tau_4, \tau_6\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$;
$\mathcal{T}^{M}_6 = \{\tau_9, \tau_{13}\}$

Задание.

Все ли наборы рубрик в первом варианте являются мультирубриками?

Определите отношения доминирования (уже, шире, несравнимо) между следующими мультирубриками:

$\mathcal{T}^{M}_1$ и $\mathcal{T}^{M}_2$; $\mathcal{T}^{M}_3$ и $\mathcal{T}^{M}_4$; $\mathcal{T}^{M}_5$ и $\mathcal{T}^{M}_6$; $\mathcal{T}^{M}_2$ и $\mathcal{T}^{M}_4$.

Постройте пересечение следующих мультирубрик II варианта:

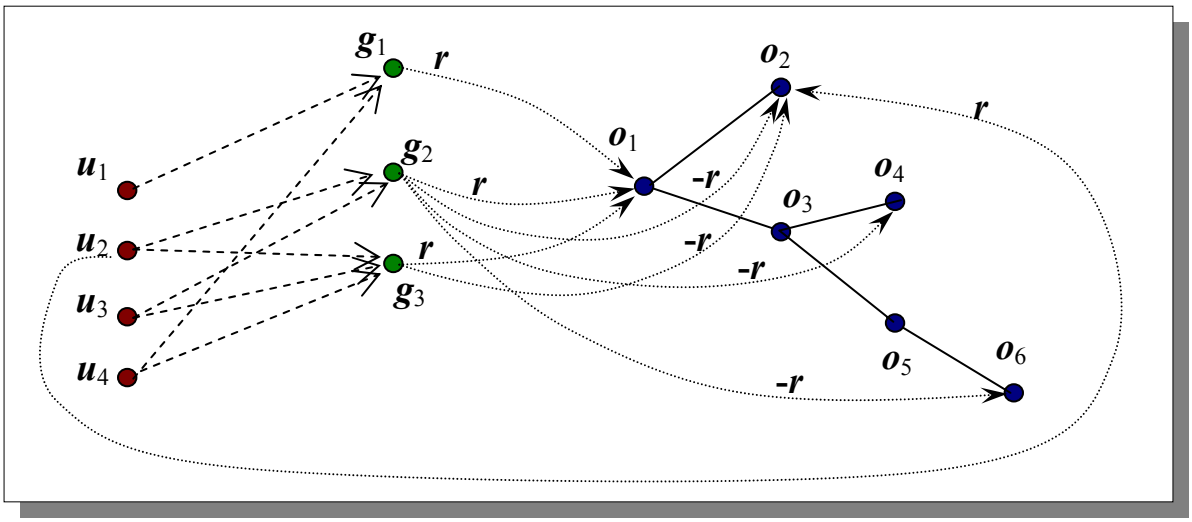
$\mathcal{T}^{M}_1 \cap_M \mathcal{T}^{M}_2$; $\mathcal{T}^{M}_2 \cap_M \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_4 \cap_M \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_1 \cap_M \mathcal{T}^{M}_6$

Билет № **12**

1. Модель типизованной матрицы доступа
2. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур".

Задача.

Пусть имеется иерархически организованная система объектов доступа, четыре пользователя $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, $\boldsymbol{u}_3$ и $\boldsymbol{u}_4$, объединенных в три рабочих группы $\boldsymbol{g}_1$, $\boldsymbol{g}_2$ и $\boldsymbol{g}_3$. Вхождение пользователей в рабочие группы, групповые и индивидуальные назначения доступа показаны на рис.



Задание. Приведите матричные соотношения и определите общий коэффициент дублирования прав доступа в системе по чтению и коэффициент дублирования прав доступа по чтению для пользователя $\boldsymbol{u}_2$.

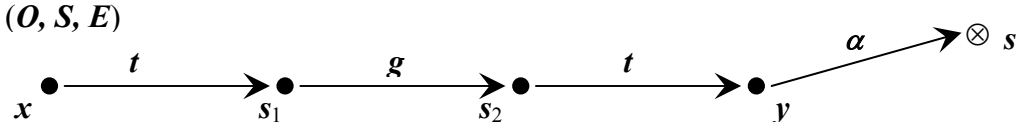
Билет № **13**

1. Основные расширения модели Белла-ЛаПадулы
2. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа

Задача.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$, в которой сущности x и y связаны tg-путем.

$\Gamma_0(O, S, E)$



Задание: построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.

Билет № **14**

1. Модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями.
2. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Количественные параметры систем индивидуально-группового доступа.

Задача.

Пусть имеется два субъекта: $\boldsymbol{s}_1$ (доверенный пользователь, *admin*) и $\boldsymbol{s}_2$ (обычный пользователь, *user*).

Пусть имеется два каталога (объекты) $\boldsymbol{o}_1$ и $\boldsymbol{o}_2$, владельцами которых являются пользователи $\boldsymbol{s}_1$ и $\boldsymbol{s}_2$, соответственно. В каталоге имеется объект $\boldsymbol{o}_3$ с секретной информацией.

Права доступа в системе заданы исходным состоянием матрицы доступа:

	$\boldsymbol{o}_1$- secret	$\boldsymbol{o}_2$ - no secret	$\boldsymbol{o}_3$ - secret
$\boldsymbol{s}_1$	*own,r,w,e*	*r,w,e*	*own,r,w,e*
$\boldsymbol{s}_2$	-	*own,r,w,e*	-

Задание. По классическому сценарию атаки с помощью троянской программы в системах, функционирующих на основе модели **HRU**, постройте систему команд перехода и соответствующие изменения матрицы доступа.

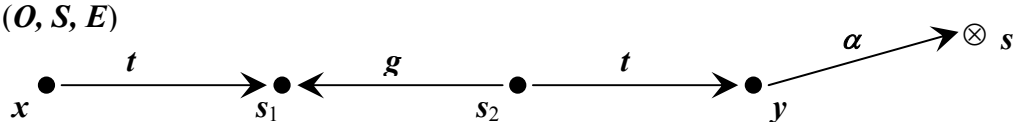
Билет № **15**

1. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах
2. Методика экспертных оценок угроз безопасности в компьютерных системах

Задача

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$, в которой сущности x и y связаны tg-путем.

$\Gamma_0(O, S, E)$



Задание: построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.

Билет № **16**

1. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона
2. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона

Задача.

Пусть имеется мандатная система доступа $\Sigma(v_0, Q, F_T)$, в которой решетка уровней безопасности Λ_L является линейной и имеет три уровня – l_1, l_2, l_3; $l_1 > l_2 > l_3$; $l_1 > l_3$.

Пусть имеется следующая система субъектов (пользователей) доступа:

u_1 – администратор системы;
u_2 – руководитель предприятия;
u_3 – делопроизводитель;
u_4 – user, т.е. рядовой непривилегированный пользователь.

Пусть имеется следующая система объектов доступа:

o_1 – системное ПО;
o_2 – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";
o_3 – документ "Приказ о поощрении работников по случаю Дня Предприятия";
o_4 – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).

Задание 1.

Обоснуйте и составьте систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа $A[u,o]$.

Составите и обоснуйте систему допусков и грифов секретности для двух состояний системы:

Состояние I – Подготовка (разработка) документа o_2.
Состояние II – Документ o_2 утвержден и введен в действие.

Является ли переход системы из состояния I в состояние II безопасным по МакЛину?